UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/332,358	06/10/1999	ENG-WHATT TOH	3915-US	2834

			EXAMINER
7590	03/29/2005		NOBAHAR, ABDULHAKIM

Cary T. Conrad
President
MESSAGE SECURE CORPORATION
24 Westech Drive
Tyngsboro, MA 01879

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

RECEIVED

APR 0 5 2005

Technology Center 2100

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 December 2004*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 12-31* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 12-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

Response to Arguments

1.   This communication is in response to applicants' amendment received on

December 23, 2004.

2.   Amendments of 1, 12, 17, and 28 and addition of claim 31 without introducing

any new matter is acknowledged.

3.   Applicants' arguments have been fully considered but they are not persuasive.

4.   Applicants in general argue that the prior art Smith does not teach a system to

store an encrypted document in escrow and in a remote device away from the sender

client and Boebert does not remedy the Smith patent deficiency in this regard.

Applicants particularly on page 15 of remarks, last paragraph argue that: "Boebert et al.

is to a non-analogous virtual private network and no one looking to cure the defects of a

delivery server system would pick and choose individual elements of transfer protocols

from a VPN to fix a mail notification system."

Boebert patent does not describe a VPN system nor it suggests applying its

method for a VPN system. On the contrary Boebert teaches "A system and method for

the secure transfer of data between a workstation connected to a private network and a

remote computer connected to an unsecured network. A secure computer is inserted

into the private network to serve as the gateway to the unsecured network and a client

subsystem is added to the workstation in order to control the transfer of data from the

workstation to the secure computer (see abstract)." Boebert particularly discusses a

system that securely transfers data such as electronic mail from one computer to

another computer over an unsecured network (see col. 6, lines 26-40; col. 9, lines 1-

10; col. 13; lines 1-6; col. 14, lines 15-24). Smith teaches "a method and system for

secure document delivery over a wide area network, such as the Internet. A document

is sent from sender to recipient via a Delivery Server. In the preferred embodiment of

the invention, the Delivery Server is directed by the sender to retrieve the intended

recipient's public key (certificate). The Delivery Server dynamically queries a certificate

authority and retrieves the public key. The public key is transmitted from the Delivery

Server to the sender (see col. 2, line 65-col. 3, line 6." Thus these two arts are

analogous.

Boebert teaches secure storage of data (i.e., encrypted data) in a facility (i.e., a

server) away from the device of the provider of data for the authorized user to access

the data (col. 6, lines 10-25; col. 12, lines 37-40; col. 14, lines 28-36; col. 29, lines 1-

10). This configuration corresponds to escrowing encrypted document in a server

separate from a sender device. Therefore, implementing the teaching of Boebert in the

system of Smith as it has been described in the last office action would meet the

limitations of the independent claims 1, 12, 17, 28 and the new claim 31.

5.   In light of the above submission examiner maintains the previous rejections of

claims including the new independent claim 31 as follows.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-10 and 12-31 are rejected under 35 USC 103(a) as being

unpatentable over Smith et al (6,061,448) (hereinafter Smith) in view of Boebert et

al (5,864,683) (hereinafter Boebert).

Claims 1-3, 5, 28 and 31

Smith discloses a system for secure document delivery over an open network,

such as Internet (col. 4, lines 26-61). The document is sent from a sender to a recipient

via a delivery sever. Smith also discloses that the document is stored on the sender's

computer (corresponding to the recited storing the package in escrow) until it is sent to

the recipient (col. 4, lines 24-35). In the Smith system, upon the sender's direction the

delivery server determines whether the recipient has a public key by querying a

database (directory) (col. 4, lines 37-49 and col. 6, lines 11-15). In the event that the

recipient does not have a public key (co. 5, lines 5-15) the server sends an e-mail

message (a notification) to the recipient containing a dynamically generated URL.

Recipient dynamically downloads (corresponding to the recited receiving an

acknowledgement from the addressee) a Java Applet or Plug-in by accessing the URL.

This Applet or Plug-in (corresponding to the recited keys generation module) then runs

on the recipient system and generates a private/public key pair. The new public key is

sent (col. 5, lines 15-29) to the delivery server. The delivery server may send the new

public key to a certificate authority for storage (a public key directory) or may simply

keep the public key in a local database. The delivery sever authenticates the public key

(corresponding to the recited authentication of the addressee). After the authentication

of the public key (corresponding to the recited in response to subsequently verified

authentication) the server transmits the recipient's public key to the sender to be used

for transmission of document to the recipient. The sender uses the authenticated

recipient's public key (col. 5, lines 30-52) to encrypt a secret key that has been used for

encryption of the document to be delivered to the recipient. Afterward, the sender

transmits the encrypted document, the recipient's address and the encrypted secret key

to the delivery server to be delivered to the recipient. In one embodiment of the Smith

system (col. 5, lines 60-65) the document encrypted by the secret key and the

encrypted secret key are delivered to the recipient. In another embodiment, the server

of the Smith system (col. 6, lines 3-10) may use the recipient's public key to encrypt the

document. The encrypted document is then transmitted to the recipient.

Smith, however, does not expressly disclose that an escrow key is used to

encrypt the document while stored in escrow on the sender's computer before delivering

to the recipient.

Boebert discloses a system of secure transfer of data from a sender to a

recipient over a public network (abstract; Fig. 12). Boebert also discloses that data is

securely stored (corresponding to the recited storing the package in escrow) by using a

local cryptography (corresponding to the recited escrow encryption key) (col. 6, lines 6-

8, col. 12, lines 39-42 and col. 28, line 47-col. 29, line 37). For delivering the data to a

client, the client is authenticated (col. 7, lines 58-64), the stored data is first decrypted

using the local cryptography and then encrypted using a negotiated cryptography

(corresponding to the recited addressee's public key) (col. 31, lines 1-41).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to implement in the system of Smith the encryption of document

using an encryption key for storing in escrow at the sender's end as taught in Boebert,

because it would protect the stored data before delivering to the recipient (col. 5, lines

8-12).

Claims 4 and 7

Claims 4 and 7 are rejected over Smith in view of Boebert as applied to the like

elements of Claims 1-3 above and further the following.

Smith (col. 4, lines 50-56) provides a secret key corresponding to the recited

escrow key, for encryption and decryption of a document (col. 3, lines 64-67) to be

transferred to a recipient. Smith also teaches that any encryption scheme (symmetric or

asymmetric) (col. 4, lines 57-67) known in the art can be utilized for the secure

transmission of information between a sender and a recipient.

Claim 6

Claim 6 is rejected over Smith in view of Boebert as applied to like elements of

Claims 1-3 above and the following.

Smith (col. 5, lines 5-15) teaches that the delivery server notifies recipient via e-

mail that there is no recipient's public key in the public key database.

Claim 8

Claim 8 is rejected over Smith in view of Boebert as applied to like elements of

Claims 1-3 above and the following.

Smith (col. 5, lines 5-15) teaches that the secret key corresponding to the recited

escrow key is not the same as the public and private keys of the recipient.

Claim 9

Claim 9 is rejected over Smith in view of Boebert as applied to like elements of

Claims 1-3 above and the following.

Smith (col. 5, lines 17-25) teaches that the server authenticates the recipient

using the recipient's e-mail address after receiving the public key of the recipient via e-

mail that includes the recipient's name and e-mail address.

Claims 10 and 15

Smith discloses that the delivery server upon the sender's request, queries a

database to retrieve the recipient's public key (col. 4, lines 39-41). The sender uses the

retrieved public key to encrypt the document (col. 3, lines 14-19). Smith also discloses

that a sender notifies a delivery server that the sender intends to send a document to a

recipient (corresponding to the recited notifying the addressee) (col. 5, lines 53-59). The

delivery sever, prior to the delivery of document, authenticates the recipient (col. 5, lines

15-29). The encrypted document is then transmitted to the recipient via a network and

only an intended recipient is permitted (an authenticated user) to gain access to the

encrypted document (col. 3, lines 52-63).

However, Smith does not disclose expressly the storing of the encrypted

document prior to the delivery of document to the recipient and authenticating the

addressee based on a message sent by the addressee.

Boebert discloses a system of secure transfer of data from a sender to a

recipient over a public network (abstract; Fig. 12). Boebert also discloses that data is

securely stored by using a local cryptography (col. 28, line 47-col. 29, line 37). Boebert

further discloses that the recipient is authenticated before sending the encrypted

document to the recipient by use of a public-key technique and digital signature

(corresponding to the authentication of addressee based on a manipulated message

sent by the addressee encrypted by the addressee's private key) (col. 4, lines 52-62).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to implement storage of an encrypted document and authentication

of the recipient prior to the delivery of the document as taught in Boebert in the system

of Smith, because it would provide for verification of the identity of the authorized

recipient (col. 5, lines 10-12).

Claims 12-14

Smith discloses a system for secure document delivery over an open network, such as Internet (col. 4, lines 26-61). The document is sent from a sender to a recipient via a delivery sever. Smith also discloses that the document is stored on the sender's computer (corresponding to the recited storing the package in escrow) until it is sent to the recipient (col. 4, lines 24-35). In the Smith system, upon the sender's direction the delivery server determines whether the recipient has a public key by querying a database (directory) (col. 4, lines 37-49 and col. 6, lines 11-15). In the event that the recipient does not have a public key (co. 5, lines 5-15) the server sends an e-mail message (a notification) to the recipient containing a dynamically generated URL. Recipient dynamically downloads (corresponding to the recited receiving an acknowledgement from the addressee) a Java Applet or Plug-in by accessing the URL. This Applet or Plug-in (corresponding to the recited keys generation module) then runs on the recipient system and generates a private/public key pair. The new public key is sent (col. 5, lines 15-29) to the delivery server. The delivery server may send the new public key to a certificate authority for storage (a public key directory) or may simply keep the public key in a local database. The delivery sever authenticates the public key (corresponding to the recited authentication of the addressee). After the authentication of the public key (corresponding to the recited in response to subsequently verified authentication) the server transmits the recipient's public key to the sender to be used for transmission of document to the recipient. The sender uses the authenticated recipient's public key (col. 5, lines 30-52) to encrypt a secret key that has been used for encryption of the document to be delivered to the recipient. Afterward, the sender

transmits the encrypted document, the recipient's address and the encrypted secret key

to the delivery server to be delivered to the recipient. In one embodiment of the Smith

system (col. 5, lines 60-65) the document encrypted by the secret key and the

encrypted secret key are delivered to the recipient. In another embodiment, the server

of the Smith system (col. 6, lines 3-10) may use the recipient's public key to encrypt the

document. The encrypted document is then transmitted to the recipient.

Smith, however, does not expressly disclose storing the document encrypted by

an escrow key and delivering the document to the recipient after decrypting the

document using the escrow key and re-encrypting the document using the recipient

public key.

Boebert discloses a system of secure transfer of data from a sender to a

recipient over a public network (abstract; Fig. 12). Boebert also discloses that data is

securely stored (corresponding to the recited storing the package in escrow) by using a

local cryptography (corresponding to the recited escrow encryption key) (col. 6, lines 6-

8, col. 12, lines 39-42 and col. 28, line 47-col. 29, line 37). For delivering the data to a

client, the client is authenticated (col. 7, lines 58-64), the stored data is first decrypted

using the local cryptography and then encrypted using a negotiated cryptography

(corresponding to the recited addressee's public key) (col. 31, lines 1-41).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to implement in the system of Smith the encryption of document

using an encryption key for storing in escrow at the sender's end, and decrypting the

document by the encryption key and re-encrypting the document using another key

such as the recipient public key prior to the delivery of the document to the recipient as

taught in Boebert, because it would protect the stored data before delivering to the

recipient (col. 5, lines 8-12).

Claims 4 and 7

Claims 4 and 7 are rejected over Smith in view of Boebert as applied to the like

elements of Claims 1-3 above and further the following.

Smith (col. 4, lines 50-56) provides a secret key corresponding to the recited

escrow key, for encryption and decryption of a document (col. 3, lines 64-67) to be

transferred to a recipient. Smith also teaches that any encryption scheme (symmetric or

asymmetric) (col. 4, lines 57-67) known in the art can be utilized for the secure

transmission of information between a sender and a recipient.

Claim 16

This claim is rejected over Smith in view of Boebert as applied to like elements of

claims 1-3 above and the following.

Smith discloses (col. 3, lines 14-18) that the document is encrypted using the

recipient public key. The encrypted document is then transmitted to the recipient and

decrypted using the new private key associated with the public key.

Claims 17 and 23

Smith discloses the use of:

An appropriate means such as Internet Lightweight Directory Access Protocol (LDAP) corresponding to the recited directory interface, to access a database in determining whether the recipient has a public key (col. 6, lines 50-65);

A computer code (corresponding to the recited notification module) that is used by the delivery server (col. 5, lines 5-11 and col. 8, lines 1-7) to send messages to the recipients via a network;

A computer module such as an applet or plug-in (corresponding to the recited a key generation module) to generate public and private keys for the recipient in response to the notification from the delivery server (col. 5, lines 10-15); and

A mechanism used by the delivery server (corresponding to the recited a transmission module) to deliver an encrypted document to a recipient (col. 5, lines 44-46 and col. 5, lines 63-67).

Smith, however, does not expressly disclose an escrow manager to provide an escrow encryption key, an encryption module to encrypt a document using the escrow key, a medium to store the encrypted document in escrow and authenticating the recipient by successful decryption of a message sent by the recipient using the public key of the addressee.

Boebert discloses a system of secure transfer of data from a sender to a recipient over a public network (abstract; Fig. 12). Boebert also discloses a local cryptography function (corresponding to the recited encryption module) either as a separate module or combined with a client protocol module that provides local cryptography such as encrypting data for securely storing locally (within internal

network) (col. 6, lines 6-10, col. 8, lines 24-42 and col. 12, lines 11-17). Boebert further

discloses authentication of the recipient before sending the encrypted document to the

recipient by use of a public-key technique (corresponding to the recited in response to

successful decryption of a message sent by addressee) (col. 4, lines 52-62 and col. 7,

lines 58-64).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to implement modules for encrypting and storing a document

locally and authenticating the recipient prior to the delivery of the document as taught in

Boebert in the system of Smith, because it would provide for protection of data and

verification of the identity of the authorized recipient (col. 5, lines 8-12).

Claim 18

This claim is rejected over Smith in view of Boebert as applied to like elements of

claim 17 above and the following.

Smith discloses the storing of the recipient's public key (col. 5, lines 25-29 and

col. 6, lines 50-67) in a database that either is residing on the delivery server or on a

separate server.

Claim 19

This claim is rejected over Smith in view of Boebert as applied to like elements of

claim 17 above and the following.

Smith discloses that the software module (applet or plug-in), after generating the public and private keys (col. 5, lines 16-29), transmits the recipient public key to the delivery server to be stored in a database for future use.

Claim 20

This claim is rejected over Smith in view of Boebert as applied to like elements of claim 17 above and the following.

Smith discloses that the delivery sever (col. 5, lines 5-11) uses a software to notify the recipient by e-mail message that there is no public key for the recipient in the database.

Claim 21

This claim is rejected over Smith in view of Boebert as applied to like elements of claim 17 above and the following.

Smith discloses that the secret key corresponding to the recited escrow key is provided to the users (col. 1, lines 33-55 and col. 7, lines 52-62) via a secure channel to be used as encryption and decryption key by the users.

Claim 22

This claim is rejected over Smith in view of Boebert as applied to like elements of claims 4 and 17 above.

Claims 24 and 25

These claims are rejected over Smith in view of Boebert as applied to like

elements of claim 17 and 23 above and the following.

Smith discloses (col. 5, lines 5-15) that the Java Applet or Plug-in (corresponding

to the recited registration module) that generates the recipient's public and private keys

is transmitted to the recipient by the delivery server in an e-mail message (attachment).

The recipient receives the said module by accessing a URL link (hyperlink).

Claim 26

This claim is rejected over Smith in view of Boebert as applied to like elements of

claim 17 and 23 above and the following.

Smith discloses (col. 7, lines 31-60 and col. 8, lines 1-10) that the delivery server

is configured to forward to the recipient the secret key corresponding to the recited

escrow key and the encrypted document. The Receive Client (a software) of the

recipient receives the document and the secret key and uses the secret key to decrypt

the document.

Claim 27

This claim is rejected over Smith in view of Boebert as applied to like elements of

claim 17 and 23 above and the following.

Smith discloses (col. 7, lines 26-30) that the Send Client (a software) of the

sender transmits to the delivery server the encrypted secret key corresponding to the

recited escrow key and the encrypted document. The delivery server may decrypt the document using the secret key and alternatively re-encrypt the document (col. 6, lines 3-5) by using the recipient's public key. The encrypted document is then sent to the recipient. The Receive Client within the recipient receives the encrypted document (col. 7, lines 35-40) and uses the recipient private key to decrypt the document.

Claim 29

Boebert discloses a system of secure transfer of data from a sender to a recipient over a public network (Fig. 12) that authenticates the recipient of the data by using a form of public-key algorithm using the private key of the recipient to encrypt a value and decrypt the value using the recipient public key (col.4, lines 53-67).

Claim 30

Boebert discloses that a notary or a local authority (corresponding to the recited certificate authority) digitally sign the public key of a private key holder i.e., issuing a certificate having some information about the holder, which corresponds to the recited making the public key available to the sender (col. 4, lines 40-52; col. 9, lines 12-28). Boebert also discloses that the recipient is authenticated based on decryption of a message using the public key of the recipient (col.4, lines 53-67).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-

272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN

March 24, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

TC2100   RANDOLPH

RETURNED TO SENDER

☑ MOVED, LEFT NO ADDRESS
☐ NOT DELIVERABLE AS ADDRESSED
UNABLE TO FORWARD
☐ ATTEMPTED - NOT KNOWN
☐ UNCLAIMED ☐ NOT KNOWN
☐ NO SUCH STREET ☐ REFUSED
☐ NO SUCH NUMBER
☐ INSUFFICIENT ADDRESS

RECEIVED

APR 0 5 2005

Technology Center 2100

UNITED STATES POSTAGE
02 1A
0004204034
MAILED FROM